A Multilayer Application-Aware IPSec Mechanism for IP Multimedia Subsystem

Chaitanya and Nirmal Roberts

***Abstract*—IP multimedia subsystem (IMS) has evolved as a platform to provide communication, multimedia and internet services in next generation network. With this unified convergence of cellular network and internet, security vulnerabilities have also increased. There is a need to protect the signaling channel as well as media stream from unauthorized access and other network attacks. In this paper we propose a multilayer application-aware IPSec mechanism having varying level of encryption for signaling and media. The use of IPSec in transport mode for securing end-to-end traffic reduces the delay and overall overhead in comparison to the hop-by-hop security mechanism adopted by 3GPP. We also propose ISKEP, a key exchange protocol for securing media plane over IP based IMS network. The security analysis shows that our technique provides mutual authentication, lawful inception, forward secrecy and protection against Replay attack..**

Index Terms—3GPP, IP multimedia subsystem, IPSec, key exchange, security.

I. Introduction

The evolution of Telecom networks to all IP network is a reality. All traffic including voice, data and multimedia services has to be converged together irrespective of the access technologies. This led to the development of IMS (IP Multimedia Subsystem) as the unifying standard Core network architecture that can address all types of terminals and all types of access methods, combining not only Internet services with communication, but also Mobile and Fixed network. With this unified convergence of cellular network and internet, security vulnerabilities have also increased. There is a need to protect the signaling channel as well as media stream from unauthorized access and other network attacks.

As specified by third-generation partnership project (3GPP), in 3G network signaling is done by session initiation protocol (SIP) and is used for IMS session establishment (setup), management and transformation [1]. SIP employs several security protocols, which may introduce additional overhead in its performance. Our aim is to provide security solution that has least overhead.

Implementation of IPSec to secure the Core Network was specified by 3GPP in [2]. They have revised the 3G Security architecture, IP network layer security and Access security for IP-based services in their Release 9 [3]-[5]. The article [6] provides an overview of 3GPP and 3GPP2 IMS and illustrates the IMS requirements, architectures, functional models and potential scalability issues.

IPSec (IP Security) is a well-known security protocol to protect internet traffic. Though IPSec provides best authentication and encryption but it has been overlooked by TLS (Transport Layer Security) and SRTP (Secure Real-time Transport Protocol), for securing signaling and media respectively in IMS core network [7]. Being at the network layer the overhead induced by IPSec header per application layer packet will be less than the transport layer security protocols and a single IPSec packet can carry multiple numbers of SIP packets reducing the overall overhead [8].

This paper proposes a multilayer application-aware IPSec which will have varying level of encryption for signaling and media. Since signaling is more vital to be protected, as a session may be hijacked by an attacking node, we will use higher level of encryption for it. As media stream is sort of encrypted due to its compression technique, it may be sent over lower level of encryption. For this we have designed a key exchange protocol. The remaining part of this paper is organized as follows. Section II briefly reviews IMS architecture and related work. Section III presents the proposed mechanism in detail. Section IV presents the security analysis of proposed mechanism. Section V has the conclusion and remarks.

II. Background and Futurework

This section describes the IMS architecture and security in brief. We first go through the 3GPP specified IMS architecture and then understand the security mechanism adopted in IMS network.

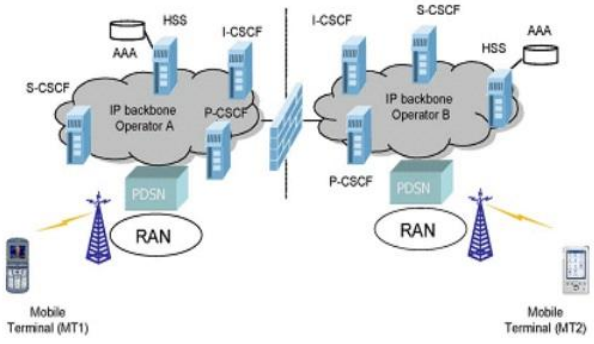

Fig. 1. IMS core network architecture [9].

A. 3GPP IMS Architecture

3GPP has adopted a layered approach to design IMS in

Manuscript received October 1, 2013; revised January 20, 2014.

The authors are with ABV-Indian Institute of Information Technology and Management, Gwalior, India. He is now with Infosys Limited, Bangalore, India (e-mail: chaitanya.singh87@gmail.com, nirmal@iiitm.ac.in).

which transport and bearer services are separated from the signaling and management. It eases the induction of new access technologies, independent of the core network. The IMS was first introduced in Release 5 of 3GPP specification and the further releases have refined its architecture. It has also become a part of the international telecommunication union (ITU) next-generation networking (NGN) vision. It provides all the network entities and procedures to support real-time voice and multimedia IP applications. It uses SIP to support signaling and session control for real-time services. The main functional entity in an IMS is the call state control function (CSCF), which is a SIP server. Depending on the specific tasks performed by a CSCF, CSCFs can be divided into three different types:

- Serving CSCF (S-CSCF): It provides session control services for a user. It is a central node of signaling layer which acts as a registrar and performs binding between subscriber and its IP address.
- Proxy CSCF (P-CSCF): It is a mobile first contact point inside an IMS and acts as a SIP Proxy Server.
- Interrogating CSCF (I-CSCF): It serves as a central contact point within an operational network for all sessions destined to a subscriber of the network or a roaming user currently visiting that network.

The home subscriber server (HSS) acts as a central repository of subscriber information. It along with authentication centre (AuC) generates and stores the security data. A function called subscriber location function (SLF) is used to locate HSS having particular user profile. Apart from registration and session control, IMS has application servers for value added services and media applications. Fig. 1 [9] illustrates the IMS core network architecture.

B. IMS Security

The IMS security mechanism consists of access security and network domain security. In access security mobile performs GPRS authentication and registration followed by packet data protocol (PDP) context activation [3].

To access the IMS services, a mobile user needs to go through following steps:

- Local P-CSCF Discovery: The mobile needs to discover the IP address of a local P-CSCF in the visited IMS because the local P-CSCF will be the mobile's first contact point in the visited IMS and the mobile's proxy for registering with the IMS. The authors of the accepted manuscripts will be given a copyright form and the form should accompany your final submission.
- Registration with IMS: The mobile needs to perform SIP registration with the visited IMS and the mobile's home IMS (which can be different from the visited IMS).

The mobile user has IMS authentication key and functions stored on a universal integrated circuit card (UICC). The collection of parameters that are used for identification, user authentication and terminal configuration is called IMS subscriber identity module (ISIM).

3GPP adopts hop-by-hop security mechanism and has five security associations numbered as per Fig. 2 [3] for IMS network.

1) The user equipment (UE) has one user private identity (IMPI) and one or more user public identity (IMPU) used for UE and HSS mutual authentication. The pre-shared long-term key in the ISIM and the authentication center (AuC) of HSS is associated with the IMPI.
2) The Gm reference point provides a security link and corresponding security associations between the UE and the P-CSCF after registration.
3) *Cx* interface provides security association for HSS database.
4) The *Za* interface provides link security for network elements between different network domains. It uses the encapsulating security payload (ESP) in tunnel mode.
5) The *Zb* interface provides link security for network elements within the same network domain.

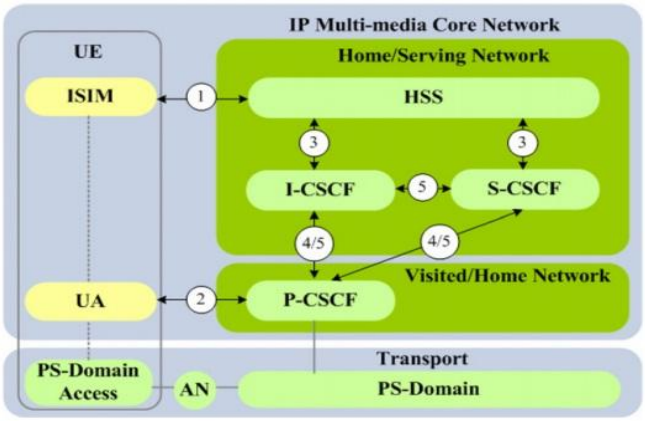

Fig. 2. IMS security architecture [3].

III. Proposed Mechanism

A. Multilayer Application-Aware IPSec

Multilayer IPSec defines a complex security relationship that involves the sender and the receiver of a security service, as well as selected intermediate nodes along the delivery path. Thus this relationship can be mapped in an all-IP wireless network. In our implementation IMS servers being the intermediate nodes are given partial access to the IP packets, i.e., they can only decrypt TCP headers for traffic management. Also the subscriber's communication data is encrypted by a key only known to the end users. The proposed scheme can be easily understood by the Fig. 3.

The above scheme uses two different keys Key1 and Key 2. Thus there has to be an application-aware key distribution technique depending on the application.

- Signaling: When the IP packet is carrying SIP requests then both keys should be same i.e. a pre shared public key with the user and corresponding secret key with the home S-CSCF server. This will facilitate the processing SIP request packets.
- Media: After signaling and authentication key exchange process the end users will share a symmetric secret Key 2. This key will be used to encrypt the media stream only. An efficient and lightweight key exchange procedure is proposed by us in next subsection.

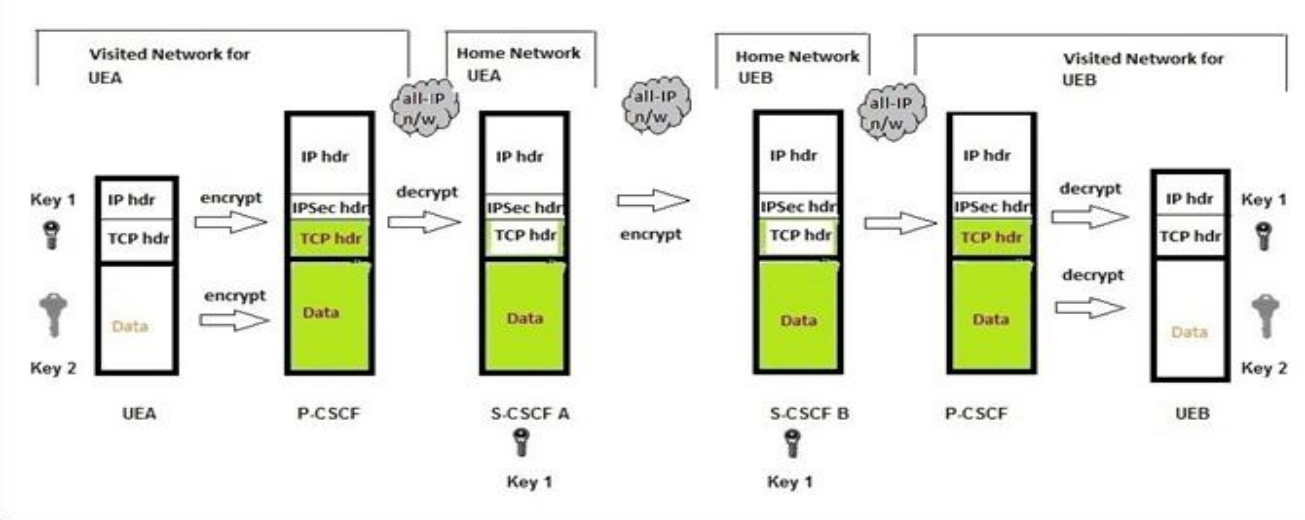

Fig. 3. Proposed technique.

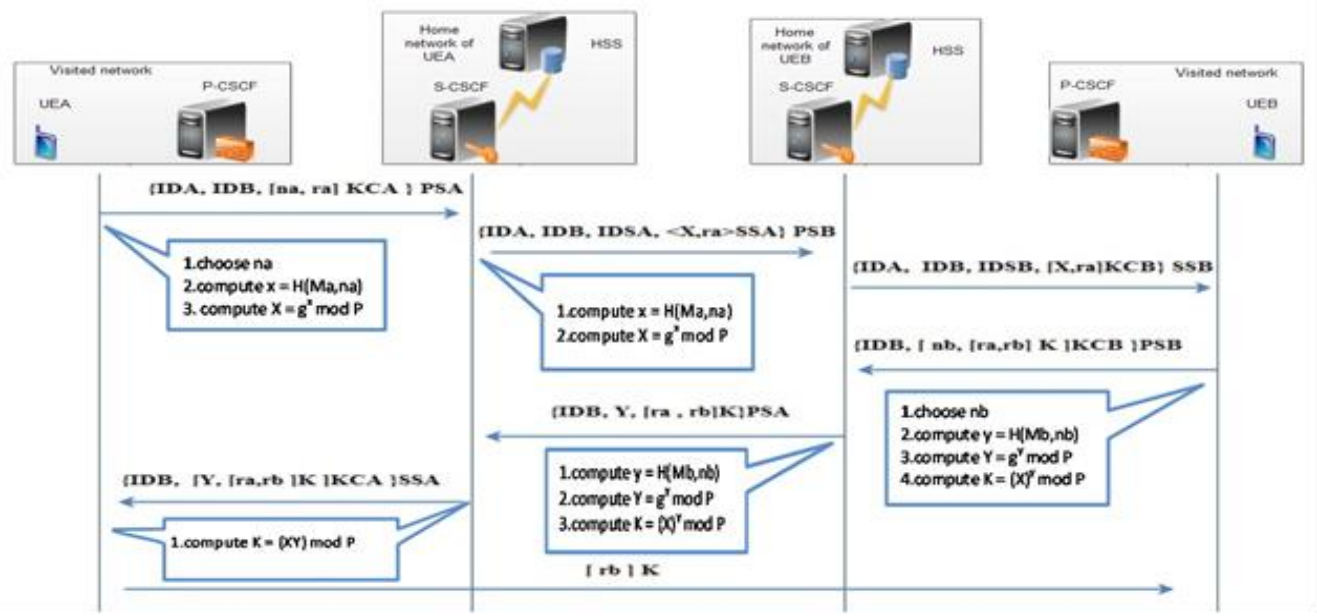

Fig. 4. ISKEP Key exchange procedure.

B. IMS Secure Key Exchange Protocol (ISKEP)

To provide end-to-end security for UEs under the IMS architecture we propose a key exchange protocol i.e. IMS Secure Key Exchange Protocol (ISKEP) to achieve the inter-domain session key exchange.

In the ISKEP, UEA and UEB respectively denote two users communicating in different IMS domains. S-CSCFA and S-CSCFB respectively denote the trusted server of UEA and UEB in the IMS domain. IDA and IDB respectively denote the identity of UEA and UEB. KCA and KCB respectively denote the Cipher keys or the Temporary Mobile Subscriber Identity (TMSI) of UEA and UEB, which only owned by users and their servers. IDSA and IDSB respectively denote the identity of S-CSCFA and S-CSCFB. SSA and PSA respectively denote the private key of S-CSCFA and the corresponding public key which known by all users successfully registered in S-CSCFA domain. SSB and PSB respectively denote the private key of S-CSCFB and the corresponding public key which known by all users successfully registered in S-CSCFB domain. The servers in IMS domain also have public keys of each other. Number p denotes a large prime number. Number g denotes a Base generator. Whereas the numbers *x*, *y*, *na*, *nb*, *ra* and *rb* are large random numbers. The message sent from UEA to UEB is denoted by $A \rightarrow B$: *M*. [Message] *K* denotes an encrypting process with symmetric key. {Message}*K* denotes an encrypting process with non-symmetric key. <Message> *K* denotes a digital signature on the message.

The proposed ISKEP protocol completes the mutual authentication and session key exchange in two round trips by embedding the keying material in SIP messages only. The detailed message exchange procedure is shown in Fig. 4.

1) UEA→S-CSCFA: {IDA, IDB, [*na*, *ra*] KCA} PSA. To share a session key with UEB, UEA firstly chooses two random numbers *na* and *ra*. It uses the pre-shared long-term key Ma and the random number *nb* as the input parameters for the one way hash function used to determine *x*, and computes the Diffe-Hellman (DH) value *X* using g^x mod *p*. UEA encrypts *na* and *ra* with the symmetrical key KCA, then encrypts IDA, IDB and [*na*, *ra*] KCA with the public key PSA of its credible server S-CSCFA.
2) S-CSCFA→S-CSCFB: {IDA, IDB, IDSA, <*X*, *ra*>SSA} PSB. After receiving message 1, S-CSCFA

decrypts message 1 with its private key SSA so that it can determine identity of the user A. Then it uses KCA to get *na* and *ra*. S-CSCFA then uses the pre-shared long-term key Ma and the random number *na* as input parameters for the one way hash function to recover *x* and computes *X* using $gx \bmod p$. After the computation phase, S-CSCFA signs the message *X*, *ra* with its private key SSA. It now encrypts IDA, IDB, IDSA and <*X*, *ra*>SSA with S-CSCFB's public key PSB, and sends the cipher texts to S-CSCFB.

3) S-CSCFB→UEB: {IDA, IDB, IDSB, [*X*, *ra*] KCB} SSB. After receiving message 2, S-CSCFB decrypts message 2 with its private key SSB to obtain information IDA, IDB, IDSA, <*X*, *ra*> SSA and verifies <*X*, *ra*> SSA with public key PSA of S-CSCFA. The response message is sent to UEB, which contains the *X* and *ra* encrypted with the KCB and also IDA, IDB, IDSB.
4) UEB→S-CSCFB: {IDB, [*nb*, [*ra*, *rb*] *K*] KCB}PSB. In the step four, UEB decrypts the message received from S-CSCFB with the public key PSB. The cypher key KCB (also working as a symmetrical key to authenticate the S-CSCFB) is used to obtain *X* and *ra*. UEB then uses the pre-shared long-term key Mb and a random number *nb* as input parameters for the to decide the *y*, and computes the DH value *Y* by $g^y \bmod p$. Furthermore, UEB obtain the session key by computing $K = X^y \bmod p$. After UEB obtained the session key *K*, it chooses a random number *rb* as the challenge number, and encrypts the *ra*, *rb* with the session key *K*. UEB then combines *nb* with the cipher texts [*ra*, *rb*] *K* using KCB encryption, and delivers it along with its identity IDB to S-CSCFB securely using public key PSB of S-CSCFB.
5) S-CSCFB→S-CSCFA: {IDB, *Y*, [*ra*, *rb*] *K*} PSA. In this step, S-CSCFB first decrypts the message with KCB to obtain the random number *nb*. S-CSCFB then uses the pre- shared long-term key Mb and the *nb* as input parameters for the recover the *y*, and computes the DH value *Y* by *gy* mod *p*. Later, S-CSCFB obtains the session key by computes *K*= *Xy* mod *p*. The message IDB, *Y*, [*ra*, *rb*] *K* is then encrypted with the S-CSCFA's public key PSA, and is sent to the S-CSCFA securely.
6) S-CSCFA→UEA: {IDB, [*Y*, [*ra*, *rb*] *K*] KCA}SSA. After receiving message 5, S-CSCFA obtains the DH value *Y* by decrypting the message with its private key SSA. S-CSCFA obtains the session key by computing *K*=(*XY*) mod *p*. S-CSCFA then combines *Y* with the cipher texts [*ra*, *rb*] *K* using KCA encryption, and delivers it along with IDB to UEA securely using its secret key SSA.
7) UEB →UEA: [*rb*] *K*. After receiving message 6, UEA decrypts the information IDB, [*Y*, [*ra*, *rb*] *K*] KCA by the public key PSA. UEA decrypts the information [*Y*, [ra,rb]*K*] KCA with the cypher key KCA and calculates the value of the session key *K*=(*XY*) mod *p*. UEA determines the identity of UEB and the effectiveness of the session key by detecting its default authentication information *ra* in the message. UEA encrypts the information *rb* with the session key K. Finally UEA transmits the cipher text called message 7 to UEB.

After successfully implementing the protocol, UEA and UEB authenticate each other and negotiate a session key $K = \{g^x\}^y \bmod p$. IMS network can use the negotiated session key to encrypt the media stream through our protocol in the duration of session establishment only.

For key exchange, the payload of a SIP message may include session description protocol (SDP) by indicating it in the Content-Type: application/sdp. SDP conveys information of media streams so prospective participants of multimedia sessions could learn the relevant setup information but we will use its field for exchanging key. The possible solution for key management extensions for SDP is specified in RFC 4567 [10]. The extensions are encoded as the SDP attributes such as (*a*=key-mgmt: IPSec), and describes which key management protocol is to be used. Therefore Media streams are protected in the IMS network without any extra transmission cost.

IV. Security Analysis

In our proposed IPSec mechanism the signaling and media plane will be protected, after UE registers with IMS network. We have taken care of several issues of IPSec to deliver lesser overload and provide best security solution. The detailed security analysis is as follows:

- We are using IPSec in transport mode with multilayer approach so that intermediate nodes can have access to TCP header for traffic processing and we can also have an end-to-end security link. Thus reducing the delay caused by adopting hop-by-hop mechanism.
- IPSec is better solution than any transport layer security protocols like TLS or SRTP and a single IPSec packet can carry multiple numbers of SIP packets reducing the overall overhead [8].
- The access network security mechanism may get redundant so we used Temporary Mobile Subscriber Identity (TMSI) which is a four-octet number in ciphered form assigned to a mobile temporarily by an MSC/VLR for circuit-switched services or by an SGSN for packet-switched services. Thus KCA and KCB in our key exchange technique is the TMSI assigned to both the UEs in GPRS authentication.
- The traffic is also reduced as key exchange message are sent in the signaling path via SDP attributes embedded over SIP messages only.
- Our mechanism provides mutual authentication between the end users as well as between the users and their respective service providers.
- 3GPP has taken account of lawful interception so our key exchange technique provides access to session keys to the service provider also, i.e., home S-CSCFs of UEs.
- An eavesdropper may replay the intercepted message to hijack a session and try to guess more information. As the DH values *X* or *Y* are computed by the UEs and S-CSCFs separately, the session key is secured from eavesdropper even if he guesses the cipher keys and the challenge numbers.
- There has to be perfect forward secrecy as the attacker can obtain the previous session key and can decrypt the challenge numbers *ra* and *rb*. But he will be helpless to guess the session key and to determine the *x* or *y* that uses a random number *na* or *nb*. As it is hard to guess the correct value from the one way hash function without the pre-shared long-term key *Ma* or *Mb*.

V. Conclusion

After examining the IPSec implementations and performances in related works, we came up with a technique to implement it as an end to end communication protocol. As per 3GPP specifications, IPSec is used along with other tunneling protocols at different interfaces of IMS, but not as complete end-to-end security protocol. We have implemented multilayer application-aware IPSec having end-to-end security association but with partial access to intermediate IMS servers. Also encryption and keying are application-aware depending on signaling or media application. Furthermore, we designed a key exchange protocol for IMS, i.e., ISKEP which provides mutual authentication, lawful inception, forward secrecy and protection against Reply attack as shown by security analysis. The main contribution of this paper is that ISKEP takes advantage of the TMSI cypher values exchanged under GPRS authentication and reduces the traffic as key exchange message are sent in the signaling path via session description protocol (SDP).

The IMS has developed as the unifying standard Core network architecture that can address all types of terminals and all types of access methods, combining not only Internet services with communication, but also Mobile and Fixed network. This transition has led to a much wider and richer service experience, there is also increased concern related to media protection and secure delivery of content that is sent over networks in digital form. Thus research and development of IMS security mechanism will be a long-term study.

References

[1] 3rd Generation Partnership Project, "IP multimedia subsystem (IMS); stage 2," *Technical Specification 3GPP TS 25.401 (V3.10.0)*, Release 99, 2000.

[2] 3rd Generation Partnership Project, "3G security; network domain security; IP network layer security," *Technical Specification 3GPP TS 33.210 (V7.3.0) Universal Mobile Telecommunications System (UMTS)*, Release 7, 2008.

[3] 3rd Generation Partnership Project, "3G security; access security for IP-based *services*," *Technical Specification Group Services and System Aspects 3GPP TS 33.203 (V9.3.0)*, Release 9, 2009.

[4] 3rd Generation Partnership Project, "3G security; security architecture," *Technical Specification Group Services and System Aspects 3GPP TS 33.102 (V9.1.0)*, Release 9, 2009.

[5] 3rd Generation Partnership Project, "3G security; IP network layer security," *Technical Specification Group Services and System Aspects 3GPP TS 33.210 (V9.0.0)*, Release 9, 2009.

[6] P. Agrawal, J. Yeh, J. Chen, and T. Zhang, "IP multimedia subsystems in 3GPP and 3GPP2: overview and scalability issues," *Communications Magazine*, vol. 46, no. 1, pp. 138–145, 2008.

[7] L. Zhang, H. Miyajima, and H. Hayashi, "An effective sip security solution for heterogeneous mobile networks," in *Proc. IEEE International Conference on Communications*, pp. 1–5, 2009.

[8] E. Cha, H. Choi, and S. Cho, "Evaluation of security protocols for the session initiation protocol," in *Proc. 16th International Conference on IEEE, Computer Communications and Networks*, pp. 611–616, 2007.

[9] H. Bao, F. Xu, and X. Huang, "Authentication key exchange protocol for IMS network," in *Proc. Power and Energy Engineering Conference (APPEEC)*, pp. 1–4, 2010.

[10] J. Arkko, F. Lindholm, E. Carrara, K. Norrman, and M. Naslund, "Key management extensions for session description protocol (SDP) and real time streaming protocol (RTSP)," RFC 4567, 2006.

Chaitanya was a research scholar at ABV-Indian Institute of Information Technology and Management, Gwalior, India, He received his master of technology degree in computer science & engineering with specialization in digital communication. The author earlier received the bachelors of technology degree in electronics and telecommunication engineering from Uttarakhand Technical University, Dehradun, India. The author's major field of study includes electronic circuits, analog & digital communication, signal processing, computer networks and information theory.

He has also worked as an intern at Opto-Electronics Factory, Ministry of Defence, dehradun, India. He is currently working with Infosys Limited, Bangalore, India. His research interests include next generation networks, IMS, LTE and mobile technologies.

Nirmal Roberts was a visiting faculty member at ABV-Indian Institute of Information Technology and Management, Gwalior, India. He has received the masters of technology degree from Indian Institute of Technology, Kanpur. The author's major field of study includes computer and network security and operating systems. The author's research interests include computer and storage networks, network management, service oriented architecture and IT infrastructure.